

WHAT IS CLAIMED IS:

1. A session shared key sharing method of sharing a session
shared key for privacy and/or authentication between a
wireless terminal that transmits and receives a packet and
5 a base station device that relays the packet when said
wireless terminal and said base station device communicate
with each other over wireless, the method comprising:

a first insertion step of inserting first information
used for creating the session shared key into the packet
10 transmitted from said wireless terminal to said base station
device based on a protocol executed when said wireless
terminal and said base station device start communicating
with each other;

a second insertion step of inserting second
15 information used for creating the session shared key into
the packet transmitted from said base station device to said
wireless terminal based on the protocol;

a first creation step of allowing said base station
device to create the session shared key based on the first
20 information inserted in the first insertion step; and

a second creation step of allowing said wireless
terminal side to create the session shared key based on the
second information inserted in the second insertion step.

2. The session shared key sharing method according to claim 1, wherein the protocol is a protocol for making a network layer address correspond to an MAC address.

5 3. The session shared key sharing method according to claim 1, wherein the protocol is an ARP, the ARP being short for Address Resolution Protocol.

10 4. The session shared key sharing method according to claim 1, wherein the protocol is a protocol for allocating a network layer address to said wireless terminal.

15 5. The session shared key sharing method according to claim 1, wherein the protocol is a DHCP, the DHCP being short for Dynamic Host Configuration Protocol.

20 6. A wireless terminal authentication method of authenticating a wireless terminal that transmits and receives a packet relayed by a base station device when said wireless terminal and said base station device communicate with each other over wireless, the method comprising:

an encryption step of enciphering first information for creating a session shared key used for the authentication using a secret key;

25 a first insertion step of inserting the first

information enciphered in the encryption step into the packet transmitted from said wireless terminal to said base station device based on a protocol executed when said wireless terminal and said base station device start communicating
5 with each other;

a decoding step of allowing said base station device to transmit the enciphered first information inserted in the first insertion step to an authentication station decoding and resending information enciphered using the
10 secret key, and to receive the first information decoded by the authentication station;

a second insertion step of inserting second information used for creating the session shared key into the packet transmitted from said base station device to said
15 wireless terminal based on the protocol;

a first creation step of allowing said base station device to create the session shared key based on the first information decoded in the decoding step; and

a second creation step of allowing said wireless
20 terminal to create the session shared key based on the second information inserted in the second insertion step.

7. The wireless terminal authentication method according to claim 6, wherein the protocol is a protocol for making
25 a network layer address correspond to an MAC address.

8. The wireless terminal authentication method according to claim 6, wherein the protocol is an Address Resolution Protocol.

5 9. The wireless terminal authentication method according to claim 6, wherein the protocol is a protocol for allocating a network layer address to said wireless terminal.

10 10. The wireless terminal authentication method according to claim 6, wherein the protocol is a Dynamic Host Configuration Protocol.

15 11. The wireless terminal authentication method according to claim 6, wherein the first information and the second information are public keys based on a Diffie-Helman type public key delivery method; and

the session shared key is a shared key based on the Diffie-Helman type public key delivery method.

20 12. The wireless terminal authentication method according to claim 6, further comprising:

a first hash value calculation step of calculating a hash value based on data including a data link layer payload of the packet transmitted from said wireless terminal to
25 said base station device and the session shared key created

in the second creation step;

a first CRC value calculation step of calculating a CRC value based on data including a MAC header and the payload of the packet and the hash value calculated in the first
5 hash value calculation step;

a packet transmission step of transmitting the packet with the CRC value calculated in the first CRC value calculation step being added to the MAC header and the payload of the packet, from said wireless terminal to said base
10 station device;

a second hash value calculation step of allowing said base station device to calculate a hash value based on data including the MAC header and the payload transmitted in the packet transmission step and the session shared key created
15 in the first creation step;

a second CRC value calculation step of calculating a CRC value based on data including the MAC header and the payload transmitted in the packet transmission step and the hash value calculated in the second hash value calculation
20 step; and

an authentication step of allowing said base station device to authenticate said wireless terminal for each packet by comparing the CRC value transmitted in the packet transmission step with the CRC value calculated in the second
25 CRC value calculation step.

13. A wireless terminal for communicating with a base station device for relaying a packet over wireless, comprising:

an insertion unit which inserts first information used
5 for creating a session shared key for privacy and/or authentication into the packet transmitted to said base station device based on a protocol executed when the wireless terminal starts communicating with said base station device;

an acquisition unit which acquires second information
10 included in the packet transmitted from said base station device based on the protocol and used for creating the session shared key; and

a creation unit which creates the session shared key based on the second information acquired by said acquisition
15 unit.

14. A wireless terminal for communicating with a base station device for relaying a packet, comprising:

an encryption unit which enciphers first information
20 used for creating a session shared key for authenticating said wireless terminal using a secret key;

an insertion unit which inserts the first information enciphered by said encryption unit into the packet transmitted to said base station device based on a protocol
25 executed when the wireless terminal starts communicating

with said base station device;

an acquisition unit which acquires second information included in the packet transmitted from said base station device based on the protocol and used for creating the session

5 shared key; and

a creation unit which creating the session shared key based on the second information acquired by said acquisition unit.

10 15. The wireless terminal according to claim 14, further comprising:

a hash value calculation unit which calculates a hash value based on data including a data link layer payload of the packet transmitted to said base station device and the
15 session shared key created by said creation unit;

a CRC value calculation unit which calculates a CRC value based on data including an MAC header and the payload of the packet and the hash value calculated by said hash value calculation unit; and

20 a packet transmission unit which transmits the packet, with the CRC value calculated by said CRC calculation unit being added to the MAC header and the payload, to said base station device.

25

16. A base station device for relaying a packet transmitted and received by a wireless terminal, comprising:

an acquisition unit which acquires first information included in the packet transmitted from said wireless terminal based on a protocol executed when said base station device starts communicating with said wireless terminal, the first information used for creating a session shared key for privacy and/or authentication;

an insertion unit which inserts second information used for creating the session shared key into the packet transmitted to said wireless terminal based on the protocol; and

a creation unit which creates the session shared key based on the first information acquired by said acquisition unit.

17. A base station device for relaying a packet transmitted and received by a wireless terminal, comprising:

an acquisition unit which acquires first information included in a packet transmitted from said wireless terminal based on a protocol executed when the base station device starts communicating with said wireless terminal, the first information enciphered by a secret key and used for creating a session shared key for authenticating said wireless terminal;

a decoding unit which transmits said enciphered first information acquired by said acquisition unit to an authentication station decoding and resending information enciphered by the secret key, and for receiving the first
5 information decoded by the authentication station;

an insertion unit which inserts second information used for creating the session shared key into the packet transmitted to said wireless terminal based on the protocol;
and

10 a creation unit which creates the session shared key based on the first information received by said decoding unit.

18. The base station device according to claim 17, further
15 comprising:

a hash value calculation unit which calculates a hash value based on data including a data link layer payload of the packet received from said wireless terminal and the session shared key created by said creation unit;

20 a CRC value calculation unit which calculates a CRC value based on data including an MAC header and the payload of the packet and the hash value calculated by said hash value calculation unit; and

an authentication unit which authenticates said
25 wireless terminal for each packet by comparing a CRC value

of the packet received from said wireless terminal with the
CRC value calculated by said CRC value calculation unit.